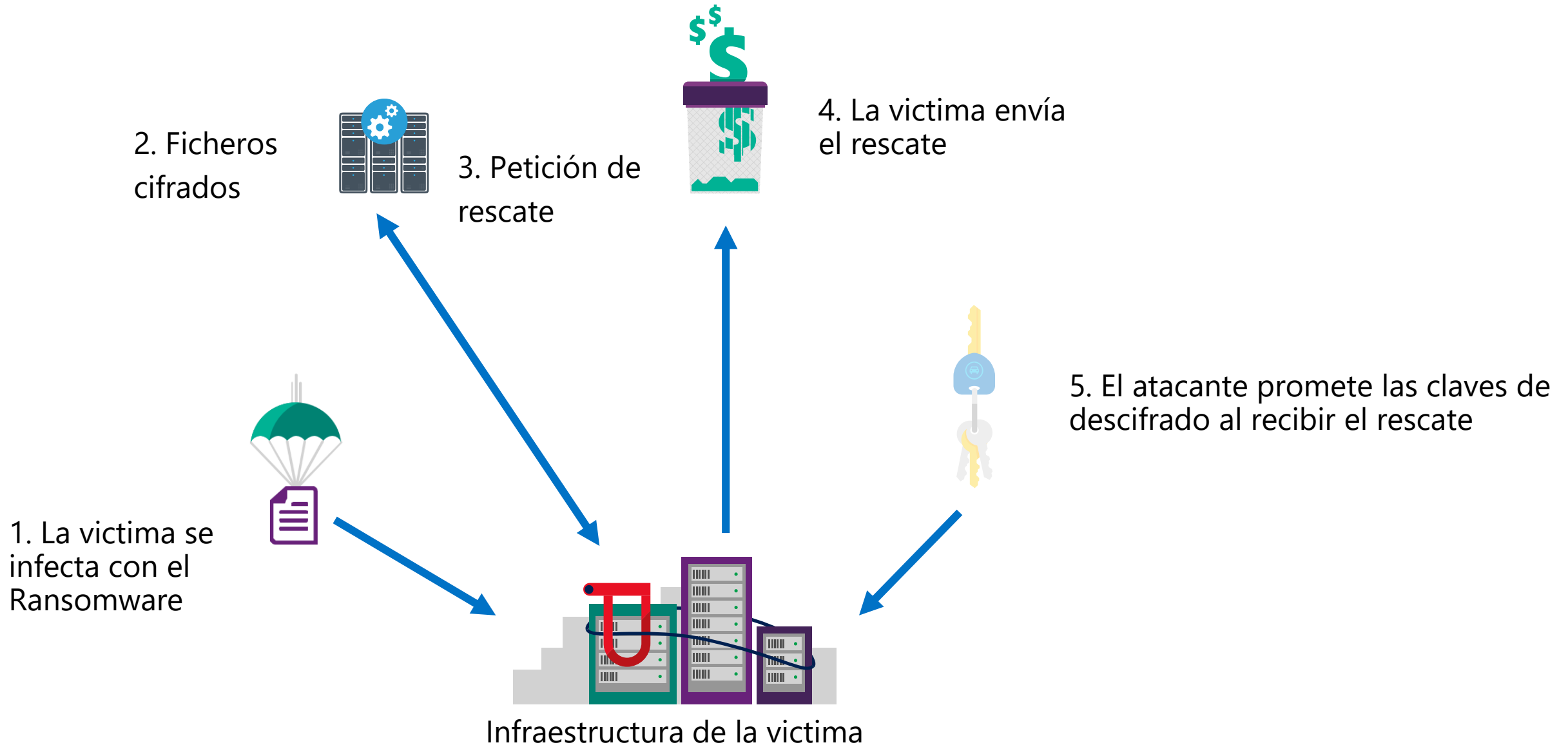


Combatiendo Ransomware

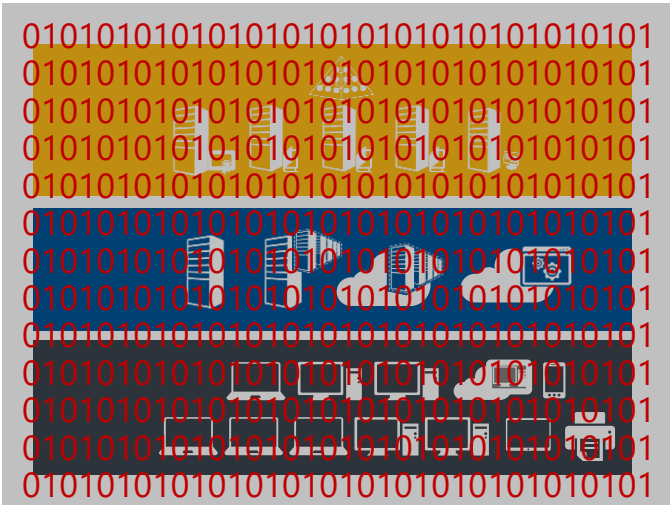
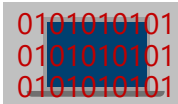
Santiago Núñez



Ransomware



Ransomware: ámbitos



Equipo/ usuario individual– *commodity malware*

- Requiere un ataque al usuario o equipo (correos spam / drive-by downloads)
- Cryptolocker/Crilock, Teslacrypt, Locky, Cryptowall
- Ransomware-as-a-Service

A toda una organización – *targeted attack*

- Requiere un ataque más complejo
 - Ataque a usuario / equipo / servidor
 - Escalado de privilegios
 - MSIL/Samas

Ataques a organizaciones



Entrada

- Dos puntos principales de entrada
 - Servidores vulnerables en Internet (confirmado)
 - Ataques a usuarios/equipos (esperado)



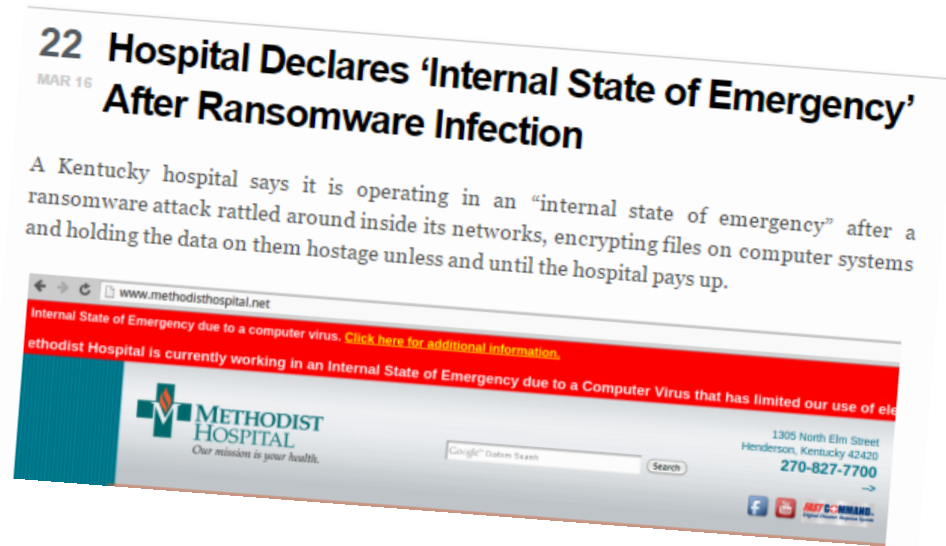
Extensión

- Similar a los "APT"
 - Recolectar contraseñas y "hashes"
 - Reconocer la red e identificar objetivos



Cifrado

- Utilizarán cifrados fuertes
 - Si llegan a cifrar el contenido, será necesario disponer de copias de seguridad no accesibles "online"



Samas infections for 6 months



#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

- 1-Public key: you need it for encryption
- 2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitocin for each affected PC to receive Private Key

Step2: After you send us one Bitcoin, Leave a comment on our blog with these de

*Your Computer name is:HQ-MS-FS-4

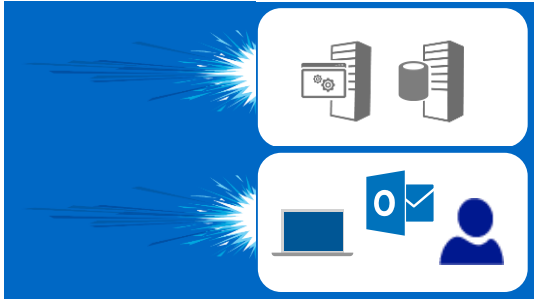
Step3: We will reply to your comment with a decryption software, You should run

*Our blog address: <http://union83939k.wordpress.com>

*Our Bitcoin address: 19CbDoaZDLTzkkTluQrMPM42AUvfQN4Kds

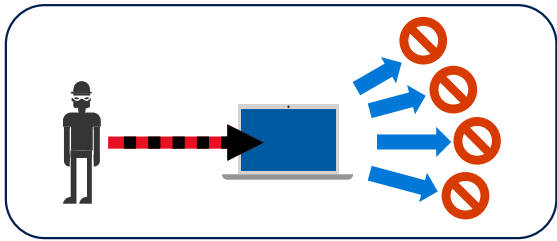
Mitigando el ransomware en nuestras organizaciones

Una aproximación práctica en tres pasos:



1. Bloquear los ataques en la entrada

- Elevar los costes de entrada para los atacantes
 - Servidores conectados a Internet
 - Equipos y usuarios



2. Defensas para contener el ataque

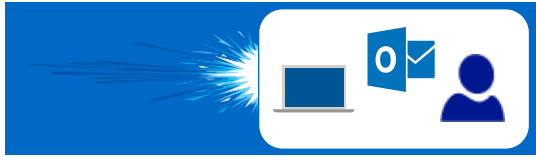
- Asumir que la primera línea de defense fallará
- Elevar los costes de extension de un atacante
- Mecanismos de respuesta rápida, detectando y bloqueando



3. Copias de seguridad

- Asumir que todas las defensas pueden fallar
- Restaurar los datos de copias de seguridad inaccesibles para los atacantes

Bloquear los ataques en la entrada



Defensas en Equipos y Usuarios

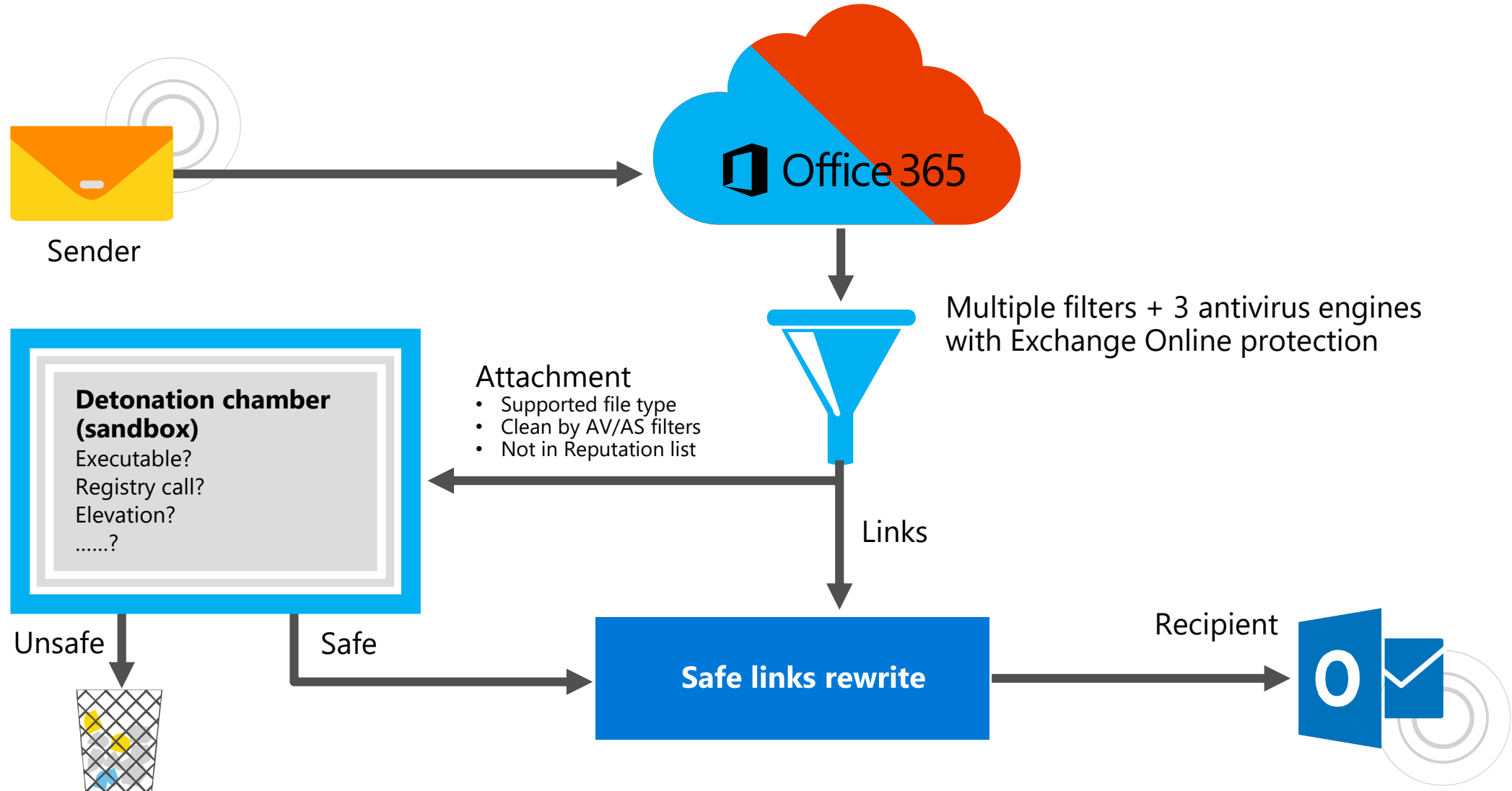
1. Protecciones en el contenido de correo y aplicaciones
2. Aplicar actualizaciones de seguridad
3. Concienciación de usuarios

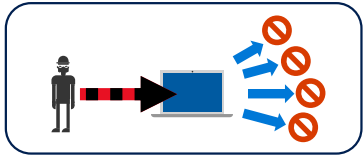


Defensas en servidores de Internet

1. Aplicar actualizaciones de seguridad (SO y Apps)
2. Higiene de operaciones (Limitar exposición de credenciales privilegiadas)
3. Higiene de configuración (Cambio de contraseñas, aplicar configuraciones)

Office 365 Advanced Threat Protection



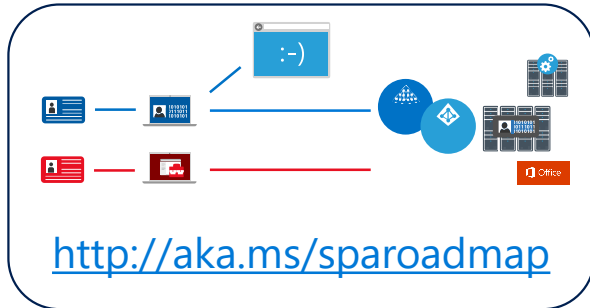


Defensas para contener el ataque



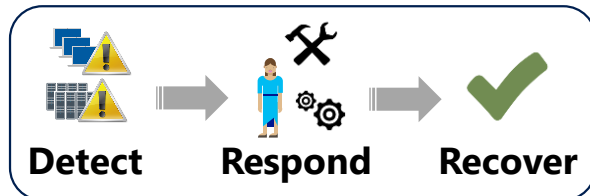
1. Eliminar los accesos excesivos a carpetas compartidas

- Eliminar los accesos para reescribir datos en recursos compartidos o SharePoint a grandes grupos (Todos, Usuarios autenticados, Usuarios de dominio, etc.)



2. Asegurar el Acceso Privilegiado

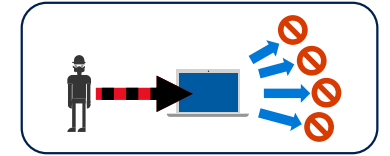
- Implementar rápidamente la fase 1 (cuentas de administración separadas, estaciones de administración dedicadas, contraseñas locales de administración aleatorias)
- Planificar fases 2 y 3



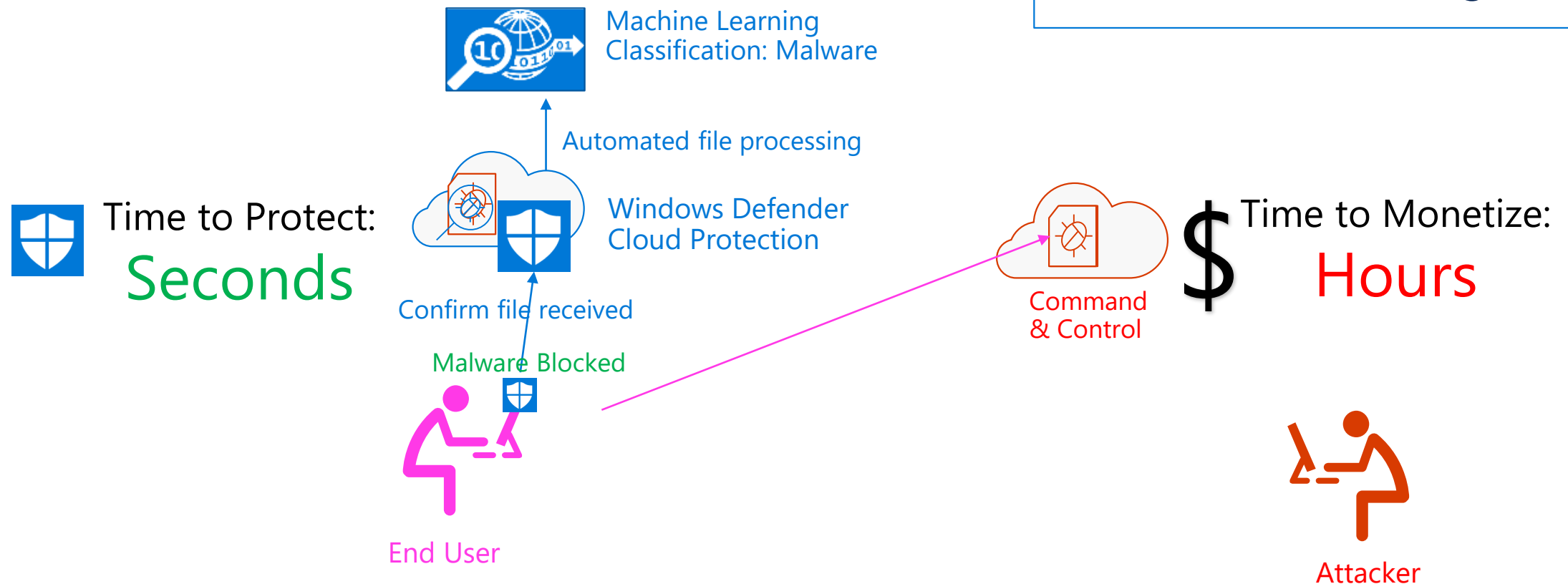
3. Operaciones de seguridad: Detección y Respuesta

- Usar capacidades anti-malware basadas en cloud para análisis y respuesta en tiempo real (Windows Defender con [Microsoft Active Protection Service \(MAPS\)](#) y [Defender ATP](#))
- Disponer de personal experimentado y preparado

Windows 10 Anniversary Update



Block at First Sight





Copias de seguridad

Estar preparados para la recuperación de un desastre

- Las copias de seguridad deben contener todos los datos críticos de negocio
- Se deben validar las copias de seguridad

Copias de seguridad inaccesibles para el atacante

- Copias de seguridad Offline
 - o
- Evitar el borrado/sobrescritura de las copias online incluso por administradores (esas credenciales pueden ser capturadas)

Servicios de nube publica como mecanismos de copia offsite

- Los accesos a la subscripción deben estar protegidos adecuadamente

Recursos

Capability	Resources
Mail and Application Content Protections	- Office 365 Exchange Online Advanced Threat Protection https://technet.microsoft.com/en-us/library/exchange-online-advanced-threat-protection-service-description.aspx - Office 2016 Internet Macro Blocking https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/ - Office 2013 VBA Macro Blocking (blocks ALL macros) https://technet.microsoft.com/en-us/library/ee857085.aspx#changevba - System Center Endpoint Protection / Windows Defender with Microsoft Active Protection Service (MAPS) https://blogs.technet.microsoft.com/mmpc/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/
Securing Privileged Access	http://aka.ms/sparoadmap
Apply Security Updates	Windows Server Update Services - https://technet.microsoft.com/en-us/windowsserver/bb332157.aspx 3rd Party application update – <varies by vendor>
Backups	Offline or otherwise attacker-inaccessible backups OneDrive for Business - https://blogs.technet.microsoft.com/office365security/how-to-deal-with-ransomware/ Azure Site Recovery – Azure Backup - https://blogs.technet.microsoft.com/hybridcloud/2016/11/04/fbi-warning-ransomware-attacks-skyrocketing/
Application Whitelisting	AppLocker - https://github.com/iadgov/AppLocker-Guidance Windows 10 Device Guard - https://technet.microsoft.com/en-us/itpro/windows/whats-new/device-guard-overview
Application Reputation	SmartScreen - http://windows.microsoft.com/en-US/internet-explorer/use-smartscreen-filter#ie=ie-11 Windows Defender with Microsoft Active Protection Service (MAPS)
Exploit Mitigations	Windows 10 Control Flow Guard - https://technet.microsoft.com/itpro/windows/keep-secure/windows-10-security-guide#secure-the-windows-core Enhanced Mitigation Experience Toolkit – http://www.microsoft.com/emet
Security Development Lifecycle (SDL)	Follow these practices for your applications and require or encourage vendors/suppliers to follow them http://www.microsoft.com/sdl
User Education	https://www.microsoft.com/en-us/security/online-privacy/phishing-symptoms.aspx

